UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

JAMES BARR, individually and on behalf of all other persons similarly situated, Plaintiff, vs. DRIZLY, LLC f/k/a DRIZLY, INC., and THE DRIZLY GROUP, INC. Defendants.	**Case No. _____** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff James Barr ("Plaintiff"), individually and on behalf of all others similarly situated, asserts the following against Defendants Drizly, LLC f/k/a Drizly, Inc. and The Drizly Group, Inc. (collectively "Drizly" or "Defendants"), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

I. INTRODUCTION

1. Plaintiff brings this Class Action Complaint on behalf of customers harmed as a result of Drizly's failure to safeguard and protect its customers' highly sensitive and personal customer information as the result of a Data Breach that has exposed Drizly's customers' information on the "dark web"—an underground or "black market" part of the internet accessed by an anonymizing browser and that is not indexed by search engines, where rampant illegal commerce occurs (e.g., buying and selling stolen card, subscription, and account information/credentials; buying and selling drugs, guns, and counterfeit money)—where it has been available to cybercriminals since *at least* February 13, 2020

2. On July 28, 2020, the online alcohol delivery service Drizly notified customers, including Plaintiff, that it had "recently identified some suspicious activity involving customer

data" and that an internal investigation had determined "that an unauthorized party appears to have obtained some of our customers' personal information" (the "Data Breach"). According to Drizly's account of the Data Breach in their email notification, the information acquired by hackers included only customer email addresses, dates of birth, passwords, and delivery addresses.

3. However, despite Drizly's claims, reporters at the leading technology industry news source *TechCrunch* quickly found that the scope and nature of the Data Breach was much broader than what Drizly had disclosed and admitted.[1] According to *TechCrunch* as many as 2.5 million Drizly accounts are believed to have been stolen.

4. *TechCrunch* obtained a portion of the data stolen as a result of the Data Breach, including several accounts of Drizly staff members, and verified the data against public records. The portion of the data that *TechCrunch* obtained also contained user phone numbers, IP addresses and geolocation data associated with the user's billing address.

5. *TechCrunch* also identified customer information from the Drizly Data Breach for sale on the dark web, where cyber criminals can purchase the information to commit fraud and identity theft, as well as other financial crimes. The post was made on February 13, 2020. Even though Drizly claimed that no customers had their financial information compromised as a result of the Data Breach, the dark web listing includes users' credit card numbers and order histories. *TechCrunch's* findings confirm that not only did Drizly allow a data breach to occur, but Drizly has failed to discover, and disclose, the full scope and extent of the Data Breach.

6. Moreover, Drizly failed to identify the breach until July 28, 2020, even though its users' sensitive customer data has been available on the dark web since at least February 13, 2020.

---

[1] Zack Whittaker, *Alcohol delivery service Drizly confirms data breach*, TECHCRUNCH (July 28, 2020), https://techcrunch.com/2020/07/28/drizly-data-breach/.

As a result of Drizly's failure to maintain reasonable security measures and protocols, Plaintiff and Class members were not provided adequate notice that their sensitive customer information was compromised for at least *five months* and were unable to take steps to proactively mitigate the harm caused by the Data Breach.

7. As Plaintiff's and Class members' sensitive customer data is currently available for purchase by cyber criminals on the dark web, they have sustained immediate, tangible injury as a direct result of the Data Breach. Plaintiff and Class members have also expended significant effort installing credit monitoring services and reviewing bank and credit card statements to mitigate the effects of the Data Breach. This injury is ongoing, as Plaintiff and Class members now face a significant and imminent risk of identity theft and fraud as demonstrated by the fact that their sensitive customer data is now available to cybercriminals for purchase on the dark web.

8. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose sensitive customer data was stolen in the Data Breach. Plaintiff and Class members seek remedies including reimbursement of losses due to identity theft and fraud and other out-of-pocket costs, compensation for time spent in response to the Data Breach, credit monitoring and identity theft insurance, and injunctive relief requiring substantial improvements to Drizly's security systems.

II. PARTIES

A. Plaintiff

9. Plaintiff James Barr is a natural person and citizen of the State of New York and a resident of New York County.

10. Plaintiff Barr has used his credit and/or debit card to make purchases utilizing the Drizly mobile application during the Data Breach period. As a result of the Data Breach, Plaintiff Barr's sensitive customer data was compromised by unauthorized third parties.

11. Had Plaintiff Barr known that Drizly would not adequately protect his sensitive customer data, he would not have made purchases using Drizly.

B. Defendants

12. Defendant Drizly, LLC f/k/a Drizly, Inc. is a limited liability company existing under the laws of the State of Delaware, with its principal place of business located at 334 Boylston Street, Suite 300, Boston, MA 02116. On December 18, 2019, Drizly, Inc. was converted into Drizly, LLC.

13. Defendant The Drizly Group, Inc. is a privately held Delaware corporation, organized and existing under the laws of the State of Delaware, with its principal place of business located at 334 Boylston Street, Suite 300, Boston, MA 02116.

14. Defendants Drizly, LLC f/k/a Drizly, Inc. and The Drizly Group, Inc. are collectively referred to throughout the Complaint as "Drizly" or "Defendants."

III. JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5 million, and many members of the class are citizens of states different from Drizly.

16. This Court has personal jurisdiction over Defendants Drizly, LLC f/k/a Drizly, Inc. and The Drizly Group, Inc. because (1) both Defendants maintain their principal places of business in Massachusetts, (2) both Defendants conduct substantial business in and throughout Massachusetts, and (3) the wrongful acts alleged in the Complaint were committed largely in Massachusetts.

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because both Drizly, LLC f/k/a Drizly, Inc. and The Drizly Group, Inc. are headquartered in this District and a

substantial part of the events giving rise to Plaintiff's claims occurred in this District. Venue is also proper because both Drizly, LLC f/k/a Drizly, Inc. and The Drizly Group, Inc. regularly transact business here.

IV. FACTUAL ALLEGATIONS

A. The Drizly Data Breach

18. According to information contained on their website, Drizly is the world's largest alcohol marketplace and the "best" way to shop for beer, wine and spirits. Drizly has become one of the biggest online alcohol delivery services in the U.S. and Canada, raising over $68 million to date, rivaling online alcohol delivery services Minibar and Delivery.com.

19. Drizly is an online mobile ordering application that partners with retail stores in over 180 geographical markets across North America to provide customers with the ability to purchase alcohol and have it delivered to them.

20. Drizly's website says "[o]ur customers trust us to be part of their lives – their celebrations, parties, dinners and quiet nights at home. We are there when it matters."

21. Despite Drizly's claims of "trust," Drizly's deficient data security measures left its customers' sensitive customer data vulnerable to hackers who pilfered this information and placed it for sale on the dark web on February 13, 2020, to which it appears Drizly was oblivious.

22. In an email to Drizly's customers (of which Plaintiff received), Drizly admitted that that it had "recently identified some suspicious activity involving customer data" and that an internal investigation had determined "that an unauthorized party appears to have obtained some of our customers' personal information."

23. On July 28, 2020, *TechCrunch* first reported that Drizly had experienced a data breach, revealing far more information about the scope and extent of the Data Breach than Drizly

provided to its customers.[2]

24. For example, according to Drizly's account of the Data Breach, the information acquired by hackers was limited to only customer email addresses, dates of birth, passwords, and delivery addresses.

25. However, according to *TechCrunch*, as many as 2.5 million Drizly accounts are believed to have been stolen. *TechCrunch* was able to obtain a portion of the data, including several accounts of Drizly staff members, and verify the data against public records. The data obtained by TechCrunch revealed that the Data Breach also included user phone numbers, IP addresses and geolocation data associated with the user's billing address, despite Drizly's claims.

26. It is important to note that Drizly has not publicly indicated *when* the hack occurred, *how long* the Data Breach lasted and its users' sensitive customer data was exposed, *when* Drizly detected and became aware of the Data Breach, or *how many* accounts were affected. But, Drizly has advised users (including Plaintiff) to change their passwords. However, an anonymous spokesperson for Drizly stated to *TechCrunch* that: "In terms of scale, up to 2.5 million accounts have been affected. Delivery address was included in under 2% of the records. And as mentioned in our email to affected consumers, no financial information was compromised."

27. Drizly's notification to Plaintiff similarly stated, "it's important to note that no financial information -- i.e. neither credit card nor debit card information -- was compromised."

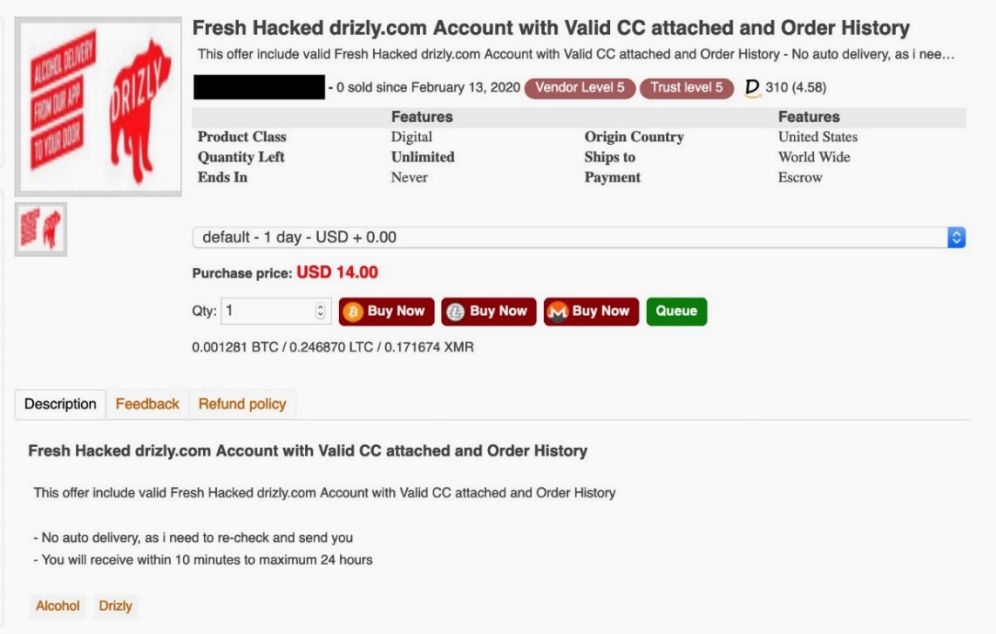
28. Drizly's account of the Data Breach appears to be a gross understatement of its scope and magnitude. For example, while Drizly has claimed that no "financial information" was taken in the Data Breach, a screen capture (Figure 1) obtained by *TechCrunch* blatantly shows the exact

---

[2] Zack Whittaker, *Alcohol delivery service Drizly confirms data breach*, TECHCRUNCH (July 28, 2020), https://techcrunch.com/2020/07/28/drizly-data-breach/.

opposite. Figure 1 below is a dark web posting from February 13, 2020 by a well-known seller of stolen credit card data. The listing offers to sell "Fresh Hacked drizly.com Account [sic] with Valid CC attached and Order History" for $14.

FIGURE 1



29. The Drizly "Fresh Hacked" post in Figure 1 demonstrates that hackers successfully exfiltrated Drizly users' sensitive customer data, including credit card numbers, resulting in the harm already sustained by Plaintiff and Class members.

30. Additionally, the "Fresh Hacked" post confirms that Plaintiff and Class members are at an significant and imminent risk of future harm of identity theft and fraud, including fraudulent charges that may be placed on customers' cards, as cyber criminals on the dark web are able to purchase their financial information and use it to commit identity theft and fraud.

31. In contrast to what is and has been frequently made available to consumers in recent data breaches, Drizly has not offered or provided any monitoring service or identity theft and fraud insurance to date despite advising Plaintiff and Class members to "reset your Drizly password,"

"continue monitoring your account for any unusual activity," and "to be extra cautious, you may want to considering changing your passwords across any sites/apps that use the same password as your Drizly account."

32. Drizly failed to properly safeguard Plaintiff's and Class members' information or timely notify them that sensitive customer data was stolen, allowing cybercriminals to access its users' sensitive customer data since *at least* February 13, 2020, when the "Fresh Hacked" dump of sensitive customer data was posted on the dark web. Drizly also failed to properly monitor its systems. Had it done so, it would have discovered the Data Breach much sooner.

33. Drizly had a continuing duty pursuant to statute, regulations, the common law, and industry standards to safeguard customers' sensitive customer data through reasonable and necessary data security measures and practices.

B. Drizly Was on Notice of a Significant Risk of a Data Breach

34. Drizly was—and at all relevant times has been—aware that the sensitive customer data that it obtains and processes is highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases.

35. Drizly also was—and at all relevant times has been—aware of the importance of safeguarding its customers' sensitive customer data and of the foreseeable consequences that would occur if its data security systems were breached, including the fraud losses and theft that would be imposed on consumers.

36. Drizly's data security obligations were particularly important and well-known given the numerous recent malware-based payment card data breaches throughout the retail and food service industry preceding the Data Breach, including breaches at Neiman Marcus, Michaels, Sally Beauty Supply, P.F. Chang's China Bistro, Eddie Bauer, Goodwill, SuperValu Grocery, UPS, Home Depot, Jimmy John's, Dairy Queen Restaurants, Staples, Kmart, Noodles & Co.,

GameStop, Wendy's, Chipotle, Arby's, Wawa, and Rutter's, which have all been widely reported by the media over the last several years. The increase in data breaches, and the risk of future breaches, is widely known throughout the retail and food service industry, including to Drizly.

37. Drizly was on notice about the risk of security infiltrations from other sources, including the U.S. Computer Emergency Readiness Team, a government unit within the Department of Homeland Security, which alerted retailers to the threat of payment system malware on July 31, 2014, and issued a guide for retailers on protecting against the threat of payment system malware, which was updated on August 27, 2014.[3] Drizly should have taken action to protect and ensure that its customers' information would not continue to be available to hackers and identity thieves, but Drizly chose not to do so.

38. Additionally, experts have long warned that the threat of hackers targeting payment system systems is serious. Well-known security expert Michael Reitblat explained in a recent trade publication that "[b]eyond POS systems, fraudsters often go directly to the source by attacking the restaurant's network or computer system, which stores files containing sensitive financial details. POS network attacks can affect multiple chain locations simultaneously and expose immense quantities of data in one fell swoop, allowing attackers to remotely steal data from each credit card as it is swiped at the cash register."[4] But, he noted that these data breaches are preventable: "[t]o help prevent fraud attacks, restaurants need to ensure they comply with the standards governing the handling of payment card information, . . . manage the risks associated with third party vendors

---

[3] *See* UNITED STATES COMPUTER EMERGENCY READINESS TEAM, ALERT (TA14-212A): BACKOFF POS MALWARE (Aug. 27, 2014), https://www.us-cert.gov/ncas/alerts/TA14-212A.

[4] Michael Reitblat, *Is your restaurant data-breach proof?*, FAST CASUAL (Aug. 3, 2018), https://www.fastcasual.com/blogs/is-your-restaurant-data-breach-proof/.

and put an effective incident response plan into place."[5]

39. These warnings, among others, put Drizly on notice that it may be susceptible to a data breach and of the importance of prioritizing data security to prevent a breach. Despite Drizly's knowledge of the likelihood that its customers' payment sensitive customer data would be stolen without reasonable security measures, Drizly failed to implement adequate data security measures that would have prevented hackers from penetrating its systems to steal sensitive customer data.

C. Drizly's Data Security Failures

40. Up to, and including, the period during which the Data Breach occurred, Drizly breached its duties, obligations, and promises to Plaintiff and Class members, by its failure to:

(a) hire qualified personnel and maintain a system of accountability over data security, thereby knowingly allowing data security deficiencies to persist;

(b) properly train its employees about the risk of cyberattacks and how to mitigate them, including by failing to implement adequate security awareness training that would have instructed employees about the risks of common techniques, what to do if they suspect such attacks, and how to prevent them;

(c) address well-known warnings that its payment system was susceptible to a data breach (*see* Section IV, B, above);

(d) implement certain protocols that would have prevented unauthorized programs, such as malware, from being installed on its systems that accessed sensitive customer data and otherwise would have protected sensitive customer data;

(e) install software to adequately track access to its network, monitor the network for unusual activity, and prevent exfiltration of data, which would have detected the presence of hackers and prevented sensitive customer data from being stolen. Specifically, there are measures that are recommended and available to prevent data from leaving protected systems and from being sent to untrusted networks outside of the corporate systems. For example, IP whitelisting, which allows only specific IP addresses to connect to trusted corporate networks and networks within the CDE, prevents hackers from sending data outside the network even when they manage to identify and collect customers' sensitive data. Similarly, system information and event monitoring ("SIEM") programs are designed to track systems activity to look

[5] *Id*.

for suspicious connections and attempts to transfer files to or from untrusted networks; and

(f) adequately safeguard consumers' sensitive customer data and maintain an adequate data security environment to reduce the risk of a data breach.

Drizly Violated PCI Data Security Standards

41. Drizly failed to comply with industry standards for data security and actively mishandled the data entrusted to it by its customers, including Plaintiff and Class members.

42. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit sensitive customer data. These standards are known as the Payment Card Industry Data Security Standard ("PCI DSS"). PCI DSS is the industry standard governing the security of sensitive customer data, although it sets the minimum level of what must be done, not the maximum.

43. PCI DSS version 3.2.1 (as described in Figure 2, below), released in May 2018 and in effect at the time of the Drizly Data Breach, imposes the following 12 "high-level" mandates:[6]

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

[6] See PCI SEC. STANDARDS COUNCIL, PCI DSS QUICK REFERENCE GUIDE: UNDERSTANDING THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD VERSION 3.2.1, at 11, (July 2018), https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf.

FIGURE 2

The PCI Data Security Standard

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data and/or sensitive authentication data. It consists of steps that mirror security best practices.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

44. Furthermore, PCI DSS 3.2.1 sets forth detailed and comprehensive requirements to be followed to meet each of the 12 mandates.

45. Among other things, PCI DSS 3.2.1 requires Drizly to: properly secure sensitive customer data; not store cardholder data beyond the time necessary to authorize a transaction; to timely upgrade its payment system software; implement proper network segmentation; encrypt sensitive customer data at the POS; restrict access to sensitive customer data to those with a need to know; establish a process to identify; and timely fix security vulnerabilities. Upon information and belief, Drizly failed to comply with some or all of these requirements.

46. As noted in the chart, PCI DSS required Drizly to "protect all systems against

malware." Drizly failed to do so. Drizly specified that it had "identified some suspicious activity involving customer data" and that "an unauthorized party appears to have obtained some of our customers' personal information…"

47. PCI DSS also required Drizly to "[t]rack and monitor all access to network resources." Drizly failed to do so. The hacker(s) had access to Drizly's system for an unspecified period of time, illustrating that Drizly had materially deficient tracking and monitoring systems in place.

48. Upon information and belief, Drizly violated numerous other provisions of the PCI DSS, including subsections underlying the chart above. Those deficiencies will be revealed during discovery with the assistance of expert witnesses.

49. PCI DSS sets the minimum level of what must be done, not the maximum. While PCI compliance is an important first step in securing cardholder data, it is not sufficient on its own to protect against all breaches, nor does it provide a safe harbor against civil liability for a data breach.

50. At all relevant times, Drizly was well-aware of its PCI DSS obligations to protect cardholder data. Drizly was an active participant in the payment card networks as it collected and likely transmitted thousands (or more) of sets of payment card data per day across 180 geographic market across 26 states.

51. Industry experts acknowledge that a data breach is indicative of data security failures. For example, research and advisory firm Aite Group has stated: "'If your data was stolen through a data breach that means you were somewhere out of compliance' with payment industry

data security standards."[7]

Drizly Violated the FTC Act

52. According to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45.

53. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

54. The FTC has also published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

55. The FTC has issued orders against businesses that have failed to employ reasonable measures to secure sensitive customer data. These orders provide further guidance to businesses

[7] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017) (accessible at: https://www.reuters.com/article/us-chipotle-cyber/chipotle-says-hackers-hit-most-restaurants-in-data-breach-idUSKBN18M2BY) (last visited August 7, 2020).

regarding their data security obligations.

56. In the years leading up to the Data Breach, and during the course of the breach itself, Drizly failed to follow guidelines set forth by the FTC and actively mishandled the management of its IT security. Furthermore, by failing to have reasonable data security measures in place, Drizly engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

D. The Data Breach Damages Plaintiff and Class Members

57. As a result of Defendants' deficient security measures and failure to timely and adequately detect the Data Breach, Plaintiff and Class members have been harmed by the compromise of their sensitive customer data in the Data Breach.

58. Plaintiff and Class members also face a substantial and imminent risk of identity theft and fraudulent charges on credit and/or debit cards. Criminals carried out the Data Breach and stole the sensitive customer data with the intent to use it for fraudulent purposes and/or to sell it, as evidenced by the dark web posting listing Drizly users' sensitive customer data available for purchase.

59. Furthermore, Plaintiff and Class members will experience an increased likelihood of identity theft and fraud going forward. This is especially true as their email addresses, dates of birth, passwords, address, phone numbers, IP addresses were compromised, and their credit card numbers are currently available for purchase by criminals on the dark web.

60. Also, many Class members will incur out of pocket costs for protective measures such as identity theft protection, credit monitoring fees, credit report fees, credit freeze fees, fees for replacement cards, and similar costs related to the Data Breach.

61. Plaintiff and Class members also suffered a "loss of value" of their credit and debit card information when it was stolen by the hacker in the Data Breach. A robust market exists for

stolen card information, which is sold on the dark web at specific identifiable prices. This market serves as a means to determine the loss of value to Plaintiff and Class members.

62. Plaintiff and Class members also suffered "benefit of the bargain" damages. Plaintiff and Class members overpaid for goods that should have been—but were not—accompanied by adequate data security. Part of the price Plaintiff and Class members paid to Drizly was intended to be used to fund adequate data security. Class members did not get what they paid for.

63. Plaintiff and Class members have spent and will continue to spend substantial amounts of time monitoring their payment card accounts for identity theft and fraud, disputing fraudulent transactions, and reviewing their financial affairs more closely than they otherwise would have done but for the Data Breach. Plaintiff and Class members will also spend time obtaining replacement cards and resetting automatic payment links to their new cards. These efforts are burdensome and time-consuming.

64. Class members who experience actual identity theft and fraud will also be harmed by the inability to use their credit or debit cards when their accounts are suspended or otherwise rendered unusable due to the fraudulent charges. To the extent Class members are charged monthly/annual fees for their credit and/or debit accounts, they are left without the benefit of that bargain while they await receipt of their replacement cards. Class members will also be harmed by the loss of use of and access to their account funds and credit lines or being limited in the amount of money they are permitted to obtain from their accounts. Class members will further be harmed by the loss of rewards points or airline mileage available on credit cards that consumers lost credit for as a result of having to use alternative forms of payment while awaiting replacement cards. This includes missed payments on bills and loans, late charges and fees, and adverse effects on

their credit, including decreased credit scores and adverse credit notations.

65. The stolen sensitive customer data is a valuable commodity to identity thieves. William P. Barr, the United States Attorney General, made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[8] The purpose of stealing large caches of sensitive customer data is to use it to defraud consumers or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit payment card fraud. Indeed, cyber criminals routinely post stolen payment card information on anonymous websites, making the information widely available to a criminal underworld. There is an active and robust market for this information. One commentator explained, "[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud."[9] Indeed, a well-known seller on the dark web has already placed Plaintiff's and Class members' stolen sensitive customer data for sale since at least February 13, 2020.

66. In the case of a data breach, merely reimbursing a consumer for a financial loss due to identity theft or fraud does not make that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[10]

---

[8] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, DEP'T OF JUSTICE, (Feb. 10, 2020) https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military.

[9] *See Legislator, security expert weigh in on Rutter's data breach*, ABC NEWS, (last updated Feb. 17, 2020 8:47 AM), https://www.abc27.com/news/local/york/legislator-security-expert-weigh-in-on-rutters-data-breach/.

[10] *See* Erika Harrell, Ph.D. and Lynn Langton, Ph.D., *Victims of Identity Theft, 2012*, U.S.

67. A victim whose payment card information has been stolen or compromised may not see the full extent of identity theft or fraud until long after the initial breach. Additionally, a victim whose payment card information has been stolen may not become aware of charges when they are nominal, as typical fraud-prevention algorithms may not capture such charges. Those charges may be repeated, over and over again, on a victim's account.

68. The risk of identity theft and fraud will persist for years. Identity thieves often hold stolen data for months or years before using it, to avoid detection. Also, the sale of stolen information on the dark web may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer. Thus, Plaintiff and Class members must vigilantly monitor their financial accounts *ad infinitum*.

E. Plaintiff and Class Members Face a Risk of Identity Theft Beyond Just Credit and Debit Card Fraud

69. Identity thieves can combine data stolen in the Data Breach with other information about Plaintiff and Class members gathered from underground sources, public sources, or even Plaintiff's and Class members' social media accounts. Thieves can use the combined data to send highly targeted phishing emails to Plaintiff and Class members to obtain more sensitive information. Thieves can use the combined data to commit potential crimes including, e.g., opening new financial accounts in Plaintiff and Class members' names, taking out loans in Plaintiff and Class members' names, using Plaintiff and Class members' information to obtain government benefits, filing fraudulent tax returns using Plaintiff and Class members' information, obtaining driver's licenses in Plaintiff and Class members' names but with another person's photograph, and giving false information to police during an arrest. Furthermore, the sensitive customer data stolen

---

Department of Justice, Bureau of Justice Statistics (Dec. 2013), at 1.

from Drizly can be used to drain debit card-linked bank accounts, make "clone" credit cards, or to buy items on certain less-secure websites.

70. Drizly has acknowledged that Plaintiff and Class members face a significant risk of various types of identity theft stemming from the Data Breach. Shifting the burden of responding to the Data Breach to consumers, Drizly recommended that affected customers undertake the following daunting tasks: "reset your Drizly password," "continue monitoring your account for any unusual activity," and "consider changing your passwords across any sites/apps that use the same password as your Drizly account."

71. Thus, by virtue of that statement, Drizly acknowledges that Plaintiff and Class members face an actual imminent risk of identity theft beyond just fraudulent credit and debit card transactions.

72. Drizly has taken no affirmative steps—beyond notifying consumers of the Data Breach—to protect against these broad-based types of identity theft and fraud, such as offering free credit monitoring and identity theft insurance to all customers whose sensitive customer data was stolen in the Data Breach. Drizly's efforts are wholly insufficient to combat the indefinite and undeniable risk of identity theft and fraud.

V. CLASS ACTION ALLEGATIONS

73. Plaintiff brings this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of a Nationwide Class.

> All persons in the United States whose sensitive customer data was compromised in the Data Breach made public by Drizly on July 28, 2020.

74. Excluded from the Class is Drizly and its subsidiaries and affiliates; all employees of Drizly and its subsidiaries and affiliates; all persons who make a timely election to be excluded

from the Class; government entities; and the judge to whom this case is assigned, including his/her immediate family and court staff.

75. Plaintiff reserves the right to modify, expand or amend the above Class definitions or to seek certification of a class or subclasses defined differently than above before any court determines whether certification is appropriate following discovery.

76. Certification of Plaintiff's claims for class-wide treatment is appropriate because all elements of Fed. R. Civ. P. 23(a) and (b)(2)-(3) are satisfied. Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in an individual action alleging the same claims.

77. **Numerosity:** All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiff is informed and believes that there are millions of members of the Class, the precise number of Class members is unknown to Plaintiff. These estimates are based on the fact that Drizly has admitted that "up to 2.5 million accounts have been affected." Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

78. **Commonality and Predominance:** All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

(a) Whether Drizly engaged in active misfeasance and misconduct alleged herein;

(b) Whether Drizly owed a duty to Class members to safeguard their sensitive customer data;

(c) Whether Drizly breached its duty to Class members to safeguard their sensitive customer data;

(d) Whether a computer hacker obtained class members' sensitive customer data in the Data Breach;

(e) Whether Drizly knew or should have known that its data security systems and monitoring processes were deficient;

(f) Whether Plaintiff and Class members suffered legally cognizable damages as a result of the Data Breach;

(g) Whether Drizly's failure to provide adequate security proximately caused Plaintiff's and class members' injuries; and

(h) Whether Plaintiff and Class members are entitled to declaratory and injunctive relief.

79. **Typicality:** All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiff is a member of the Class. Plaintiff's claims are typical of the claims of all Class members because Plaintiff, like other Class members, suffered a theft of his sensitive customer data in the Data Breach.

80. **Adequacy of Representation:** All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiff is an adequate Class representative because he is members of the class and his interests do not conflict with the interests of other class members that he seeks to represent. Plaintiff is committed to pursuing this matter for the class with the class's collective best interests in mind. Plaintiff has retained counsel competent and experienced in complex class action litigation of this type and Plaintiff intends to prosecute this action vigorously. Plaintiff, and his counsel, will fairly and adequately protect the class's interests.

81. **Predominance and Superiority:** All requirements of Fed. R. Civ. P. 23(b)(3) are satisfied. As described above, common issues of law or fact predominate over individual issues. Resolution of those common issues in Plaintiff's case will also resolve them for the class's claims. In addition, a class action is superior to any other available means for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff

and other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Drizly, so it would be impracticable for members of the Class to individually seek redress for Drizly's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

82. **Cohesiveness:** All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Drizly has acted, or refused to act, on grounds generally applicable to the Class such that final declaratory or injunctive relief appropriate.

VI. CHOICE OF LAW

83. The common law of Massachusetts governs Plaintiff's claims.

84. Drizly's acts and omissions discussed herein were orchestrated and implemented at its corporate headquarters in Massachusetts and the tortious and deceptive acts complained of occurred in, and radiated from, Massachusetts.

85. The key wrongdoing at issue in this litigation—Drizly's failure to employ adequate data security measures—emanated from Drizly's headquarters in Massachusetts.

86. Upon information and belief, control over Drizly's payment systems and IT personnel is exercised at its headquarters in Massachusetts.

87. Massachusetts, which seeks to protect the rights and interests of Massachusetts residents and other residents against a company doing business in Massachusetts, has a greater interest in Plaintiff's and Class members' claims than any other state and is most intimately concerned with the outcome of this litigation.

88. Application of Massachusetts law to a nationwide Class with respect to Plaintiff's and Class members' claims is neither arbitrary nor fundamentally unfair because Massachusetts has a significant aggregation of contacts that creates a state interest in Plaintiff's and Class members' claims.

89. To the extent that there is a dispute concerning choice of law, such a dispute may be briefed after substantial discovery is completed.

VII. CAUSES OF ACTION[11]

COUNT I
NEGLIGENCE

90. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

91. Drizly obtained Plaintiff's and Class members' sensitive customer data in connection with class members' purchases on Drizly.

92. By collecting and maintaining sensitive customer data, Drizly had a duty of care to use reasonable means to secure and safeguard the sensitive customer data and to prevent disclosure of the information to unauthorized individuals. Drizly's duty included a responsibility to implement processes by which it could detect a data breach of this type and magnitude in a timely manner.

93. Drizly owed a duty of care to Plaintiff and Class members to provide data security consistent with the various requirements and rules discussed above.

[11] Plaintiff sent a demand letter to Defendants pursuant to Mass. G. L. Ch. 93A on the date of the filing of this Complaint. Should the good-faith negotiations resulting from the letter be unsuccessful, Plaintiff reserves the right to amend the complaint to add a claim under 93A.

94. Drizly's duty of care arose as a result of, among other things, the special relationship that existed between Drizly and its customers. Drizly was the only party in a position to ensure that its systems were sufficient to protect against the foreseeable risk that a data breach could occur, which would result in substantial harm to consumers.

95. Also, Drizly had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to use reasonable measures to protect confidential consumer data.

96. Drizly's duty to use reasonable care in protecting cardholder data arose as a result of the common law, statutes, and regulations described above, but also because Drizly is bound by industry standards and PCI DSS rules to protect sensitive customer data.

97. Drizly was subject to an "independent duty" untethered to any contract between Plaintiff and Class members and Drizly.

98. Drizly breached its duties, and thus was negligent, by failing to use reasonable measures to protect cardholder information. Drizly's negligent acts and omissions include, but are not limited to, the following:

(a) failure to delete cardholder information after the time period necessary to authorize the transaction;

(b) failure lure to employ systems and educate employees to protect against malware;

(c) failure to comply with industry standards for software and payment system security;

(d) failure to track and monitor access to its network and cardholder data;

(e) failure to limit access to those with a valid purpose;

(f) failure to adequately staff and fund its data security operation;

(g) failure to use due care in hiring, promoting, and supervising those responsible for its data security operations; and

(h) failure to recognize that hackers were stealing sensitive customer data from its network while the Data Breach was taking place.

99. It was foreseeable to Drizly that a failure to use reasonable measures to protect sensitive customer data could result in injury to consumers. Further, actual and attempted breaches of data security were reasonably foreseeable to Drizly given the known frequency of payment card data breaches and various warnings from card brands and industry experts.

100. Plaintiff and Class members suffered various types of damages as alleged above.

101. Drizly's wrongful conduct was a proximate cause of Plaintiff's and Class members' damages.

102. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

103. Plaintiff and Class members are also entitled to injunctive relief requiring Drizly to (among other things): (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide several years of free credit monitoring and identity theft insurance to all Class members.

COUNT II
NEGLIGENCE *PER SE*

104. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

Negligence *Per Se* Pursuant to the FTC Act, 15 U.S.C. § 45

105. As alleged above, pursuant to the FTC Act, 15 U.S.C. § 45, Drizly had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' sensitive customer data.

106. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Drizly, of failing to use reasonable measures to protect sensitive customer data. The FTC publications and orders described above also form part of the basis of Drizly's duty.

107. Drizly violated Section 5 of the FTC Act by failing to use reasonable measures to protect sensitive customer data and not complying with applicable industry standards, including PCI DSS, as described in detail herein. Drizly's conduct was particularly unreasonable given the nature and amount of sensitive customer data it collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to consumers.

108. Plaintiff and members of the Class are within the class of persons that Section 5 of the FTC Act was intended to protect, because the FTC Act was expressly designed to protect consumers from "substantial injury."

109. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class members.

110. Drizly had a duty to Plaintiff and Class members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class members' sensitive customer data.

111. Drizly breached its duties to Plaintiff and Class members under the FTC Act, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' sensitive customer data.

112. Drizly's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

113. But for Drizly's wrongful and negligent breach of its duties owed to Plaintiff and class members, Plaintiff and Class members would not have been injured.

114. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Drizly's breach of its duties. Drizly knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and Class members to suffer the foreseeable harms associated with the exposure of their sensitive customer data.

115. Had Plaintiff and Class members known that Drizly did and does not adequately protect customer sensitive customer data, they would not have made purchases on Drizly.

116. As a direct and proximate result of Drizly's negligence *per se*, Plaintiff and Class members have suffered harm, including but not limited to loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Drizly that Plaintiff and Class members would not have made had they known of Drizly's careless approach to cyber security; lost control over the value of sensitive customer data; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen sensitive customer data, entitling them to damages in an amount to be proven at trial.

Negligence *Per Se* Pursuant to the Massachusetts Data Security statute, Mass. Gen. Laws Ann. ch. 93H, § 1 *et seq.*, and the Standards for The Protection of Personal Information of Residents of The Commonwealth Regulations, 201 Mass. Code Regs. 17.01 *et seq.*

117. Pursuant to Mass. Gen. Laws Ann. ch. 93H, §1 *et seq.* and 201 Mass. Code Regs. § 17.01 *et seq.*, Drizly not only had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' sensitive customer data, but also a duty "as soon as practicable and without unreasonable delay" to send the proper notification to Massachusetts authorities and affected residents.

118. Mass. Gen. Laws Ann. ch. 93H, § 2(a) has two principal components.

119. The first component enables various branches of the state government to adopt privacy rules and regulations to:

> insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

Mass. Gen. Laws Ann. ch. 93H, § 2(a). The executive branch of the state government has responded by promulgating "Standards for the Protection of Personal Information of Residents of the Commonwealth." 201 Mass. Code Regs. §§ 17.01–17.05. These standards impose duties and requirements on persons and entities that own, license, or maintain personal information about Massachusetts residents. *Id.* §§ 17.03–17.04.

120. The second component of Mass. Gen. Laws Ann. ch. 93H establishes privacy notification requirements. Mass. Gen. Laws Ann. ch. 93H, § 3. These requirements are triggered by any "breach of security," as defined by the statute, or any unauthorized access or use of personal information. *Id.* §§ 1(a), 3. When such unauthorized access or use occurs, persons and entities that own, license, or maintain Massachusetts residents' personal information must provide notice to the Massachusetts Attorney General, the Massachusetts Director of Consumer Affairs and Business Regulation. and affected parties pursuant to various disclosure guidelines. *Id.* §3(b).

121. Under 201 Mass. Code Regs. § 17.02, Drizly is a "person."

122. Under 201 Mass. Code Regs. § 17.02, Drizly "owns or licenses" the "personal information" of Plaintiff and Class members, which includes "receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services…"

123. Under 201 Mass. Code Regs. § 17.02, "personal information," includes "a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account."

124. 201 Mass. Code Regs. §§ 17.03 – 17.04 outline Drizly's duties to protect "personal information," the standards for protecting "personal information," as well as requisite computer system security requirements.

125. 201 Mass. Code Regs. § 17.05 requires that "[e]very person who owns or licenses personal information about a resident of the Commonwealth shall be in full compliance with 201 CMR 17.00 on or before March 1, 2010."

126. Drizly violated Mass. Gen. Laws Ann. ch. 93H, § 2 and the accompanying regulations of 201 Mass. Code Regs. § 17.01 *et seq.* by failing to use reasonable measures to protect sensitive customer data and "personal information," as well as not complying with the applicable standards enumerated in the statute and regulations. Drizly's conduct was particularly unreasonable given the nature and amount of sensitive customer data and "personal information,"

it collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to consumers.

127. Drizly violated Mass. Gen. Laws Ann. ch. 93H, § 3 since it was required to send notice "as soon as practicable and without unreasonable delay" to the Massachusetts Attorney General, the Massachusetts Director of Consumer Affairs and Business Regulation, and to resident, "when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose…"

128. Drizly's notification email to Plaintiff stated that their "investigation is ongoing" and that Drizly "engaged a cyber security firm to help us identify all affected parties." This indicates that Drrizly has yet to fully grasp the scope of the Data Breach and is negligent in its reporting requirements for Massachusetts residents. Mass. Gen. Laws Ann. ch. 93H, § 3(b) requires that the notification to the Massachusetts Attorney General and the Massachusetts Director of Consumer Affairs and Business Regulation "identify the number of residents of the commonwealth affected by such incident at the time of notification."

129. The most recent "Data Breach Notification Report" published by the Office Consumer Affairs and Business Regulation is current as of July 29, 2020 and does not list the Drizly Data Breach, which was first reported by *TechCrunch* on July 28, 2020. Upon information and belief, Drizly sent its notification email to affected users on or about July 28, 2020 as well.

130. Mass. Gen. Laws Ann. ch. 93H, § 3(b) further provides that the notice to the Massachusetts Attorney General and the Massachusetts Director of Consumer Affairs and Business Regulation "shall not be delayed on grounds that the total number of residents affected is not yet ascertained."

131. The harm that has occurred is the type of harm the Massachusetts Data Security statute (Mass. Gen. Laws Ann. ch. 93H, § 1 *et seq.*) and the Standards for The Protection of Personal Information of Residents of The Commonwealth regulations (201 Mass. Code Regs. 17.01 *et seq.*) is intended to guard against.

132. Drizly had a duty to Plaintiff and Class members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class members' sensitive customer data and "personal information."

133. Drizly breached its duties to Plaintiff and Class members under the Massachusetts Data Security statute (Mass. Gen. Laws Ann. ch. 93H, § 1 *et seq.*) and the Standards for The Protection of Personal Information of Residents of The Commonwealth regulations (201 Mass. Code Regs. § 17.01 *et seq.*), by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' sensitive customer data and "personal information.".

134. Drizly's violation of Massachusetts Data Security statute (Mass. Gen. Laws Ann. ch. 93H, § 1 *et seq.*) and the Standards for The Protection of Personal Information of Residents of The Commonwealth regulations (201 Mass. Code Regs. § 17.01 *et seq.*), and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

135. But for Drizly's wrongful and negligent breach of its duties owed to Plaintiff and Class members, Plaintiff and Class members would not have been injured, or would not have been injured to as great a degree.

136. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Drizly's breach of its duties. Drizly knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and Class members to suffer the

foreseeable harms associated with the exposure of their sensitive customer data and "personal information."

137. Had Plaintiff and Class members known that Drizly did and does not adequately protect customer sensitive customer data and "personal information" they would not have made purchases using Drizly.

138. As a direct and proximate result of Drizly's negligence *per se*, Plaintiff and Class members have suffered harm, including but not limited to loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Drizly that Plaintiff and Class members would not have made had they known of Drizly's careless approach to cyber security; lost control over the value of sensitive customer data; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen sensitive customer data and "personal information," entitling them to damages in an amount to be proven at trial.

Negligence *Per Se* Pursuant to the Shield Act, N.Y. Gen. Bus. Law § 899-aa *et seq.*

139. Pursuant to N.Y. Gen. Bus. Law § 899-aa *et seq.* (known as the "Shield Act"), Drizly not only had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' sensitive customer data, "private information," and "personal information," but also a duty to send notification to the affected New York resident "in the most expedient time possible and without unreasonable delay."

140. N.Y. Gen. Bus. Law § 899-aa(2), provides that [a]ny person or business which owns or licenses computerized data which includes *private information* shall disclose any *breach*

of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay…" (emphasis added).

141. Under N.Y. Gen. Bus. Law § 899-aa(1)(c), "Breach of the security of the system" "shall mean unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business."

142. Under N.Y. Gen. Bus. Law § 899-aa(1)(b), "Private information" "shall mean either: (i) *personal information* consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired:

> (3) account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account;
>
> (4) account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or
>
> (5)(ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

143. Under N.Y. Gen. Bus. Law § 899-aa(1)(a), "Personal information" "shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person."

144. Under N.Y. Gen. Bus. Law § 899-aa(5)(d)(1), e-mail notice to affected residents are permitted when such business has an e-mail address for the subject persons, "**except if the**

breached information includes an e-mail address in combination with a password or security question and answer **that would permit access to the online account**, in which case the person or business shall instead provide clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an internet protocol address or from an online location which the person or business knows the consumer customarily uses to access the online account." The sensitive customer data exposed in the Data Breach included "email addresses" and "password." Thus, Drizly's email notification to Plaintiff was in violation of N.Y. Gen. Bus. Law § 899-aa(5)(d)(1), since a "clear and conspicuous notice" sent to Plaintiff online where Plaintiff would be connected to an online account from an internet protocol address or from an online location which the person or business knows the consumer customarily uses to access the online account was never provided to Plaintiff.

145. Under N.Y. Gen. Bus. Law § 899-bb(2)(a), "[a]ny person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data." The data security protections Drizly was obligated to undertake are enumerated at N.Y. Gen. Bus. Law § 899-bb(2)(b) *et seq.*

146. Under N.Y. Gen. Bus. Law § 899-bb(2)(d), "[a]ny person or business that fails to comply with this subdivision shall be deemed to have violated section three hundred forty-nine of this chapter," which is New York General Business Law, N.Y. Gen. Bus. Law § 349, *et seq.*

147. The harm that has occurred is the type of harm the N.Y. Gen. Bus. Law § 899-aa *et seq.* (the "Shield Act") is intended to guard against.

148. Drizly had a duty to Plaintiff and Class members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class members' sensitive customer data, "private information," and "personal information."

149. Drizly breached its duties to Plaintiff and Class members under N.Y. Gen. Bus. Law § 899-aa *et seq.* (the "Shield Act"), by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' sensitive customer data, "private information," and "personal information."

150. Drizly's violation of N.Y. Gen. Bus. Law § 899-aa *et seq.* (the "Shield Act") and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

151. But for Drizly's wrongful and negligent breach of its duties owed to Plaintiff and Class members, Plaintiff and Class members would not have been injured, or would not have been injured to as great a degree.

152. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Drizly's breach of its duties. Drizly knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and Class members to suffer the foreseeable harms associated with the exposure of their sensitive customer data, "private information," and "personal information."

153. Had Plaintiff and Class members known that Drizly did and does not adequately protect customer sensitive customer data, "private information," and "personal information," they would not have made purchases using Drizly.

154. As a direct and proximate result of Drizly's negligence *per se*, Plaintiff and Class members have suffered harm, including but not limited to loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft;

financial losses related to the purchases made at Drizly that Plaintiff and Class members would not have made had they known of Drizly's careless approach to cyber security; lost control over the value of sensitive customer data; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen sensitive customer data, "private information," and "personal information," entitling them to damages in an amount to be proven at trial.

155. Drizly's violation of N.Y. Gen. Bus. Law § 899-bb is a *per se* violation of N.Y. Gen. Bus. Law § 349, *et seq*.

COUNT III
BREACH OF IMPLIED CONTRACT

156. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

157. When Plaintiff and Class members provided their sensitive customer data to Drizly in exchange for Drizly's products, they entered into implied contracts with Drizly under which Drizly agreed to take reasonable steps to protect the sensitive customer data.

158. Drizly solicited and invited Plaintiff and Class members to provide their sensitive customer data as part of Drizly's regular business practices. Plaintiff and Class members accepted Drizly's offers and provided their sensitive customer data to Drizly.

159. When entering into the implied contracts, Plaintiff and Class members reasonably believed and expected that Drizly's data security practices complied with relevant laws, regulations, and industry standards.

160. Plaintiff and Class members paid money to Drizly to purchase items on Drizly. Plaintiff and Class members reasonably believed and expected that Drizly would use part of those funds to obtain adequate data security. Drizly failed to do so.

161. Plaintiff and Class members would not have provided their sensitive customer data to Drizly in the absence of Drizly's implied promise to keep the sensitive customer data reasonably secure.

162. Plaintiff and Class members fully performed their obligations under the implied contracts by paying money to Drizly.

163. Drizly breached its implied contracts with Plaintiff and Class members by failing to implement reasonable data security measures.

164. As a direct and proximate result of Drizly's breaches of the implied contracts, Plaintiff and Class members sustained damages as alleged herein.

165. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

COUNT IV
UNJUST ENRICHMENT

166. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

167. This claim is plead in the alternative to the above implied contract claim.

168. Plaintiff and Class members conferred a monetary benefit upon Drizly in the form of monies paid for the purchase of items on Drizly.

169. Drizly appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class members. Drizly also benefited from the receipt of Plaintiff's and Class members' sensitive customer data as this was utilized by Drizly to facilitate payment to it.

170. The monies Plaintiff and Cass members paid to Drizly were supposed to be used by Drizly, in part, to pay for adequate data privacy infrastructure, practices, and procedures.

171. As a result of Drizly's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their purchases made with adequate data privacy and security practices and procedures that Plaintiff and Class members paid for, and those purchases without adequate data privacy and security practices and procedures that they received.

172. Under principals of equity and good conscience, Drizly should not be permitted to retain the money belonging to Plaintiff and Class members because Drizly failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

173. Drizly should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

VIII. RELIEF REQUESTED

Plaintiff, on behalf of all others similarly situated, request that the Court enter judgment against Drizly including the following:

A. Determining that this matter may proceed as a class action and certifying the Classes asserted herein;

B. Appointing Plaintiff as representative of the applicable Classes and appointing Plaintiff's counsel as class counsel;

C. An award to Plaintiff and the Classes of compensatory, consequential, statutory, and treble damages as set forth above;

D. Ordering injunctive relief requiring Drizly to (among other things): (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide several years of free credit monitoring and identity theft insurance to all Class members;

E. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

F. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

G. Such other relief as the Court may allow.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury trial all issues so triable.

August 7, 2020

Respectfully submitted,

/s/ Jacob A. Walker
Jason M. Leviton (BBO #678331)
Jacob A. Walker (BBO #688074)
BLOCK & LEVITON LLP
260 Franklin Street, Suite 1860
Boston, MA 02110
(617) 398-5600
jason@blockleviton.com
jake@blockleviton.com

Christian Levis (*pro hac vice* forthcoming)
Amanda Fiorilla (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel: (914) 997-0500
Fax: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com

Anthony M. Christina (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Tel: (215) 399-4770
Fax: (914) 997-0035
achristina@lowey.com

Gary F. Lynch (*pro hac vice* forthcoming)
Jamisen A. Etzel (*pro hac vice* forthcoming)
CARLSON LYNCH, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
glynch@carlsonlynch.com
jetzel@carlsonlynch.com